



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,441	12/27/2000	Wolfgang Daum	9D-HR-19614-Daum et al	4179

7590

03/23/2005

John S. Beulick
Armstrong Teasdale LLP
ONE METROPOLITAN SQUARE
SUITE 2600
ST. LOUIS, MO 63102

EXAMINER

DINH, MINH

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/748,441

Applicant(s)

DAUM ET AL.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 November 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) 1-15 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 16-20 and 23-31 is/are rejected.
- 7) ☒ Claim(s) 21 and 22 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 July 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/15/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. The application has been amended as follows: claims 1-15 have been withdrawn; claims 16, 20-21, 25 and 27-30 have been amended.
2. A copy of the IDS filed 07/15/2004 is provided with this Office Action. The delay in providing the copy is regretted.

Response to Arguments

3. Applicant's traversal filed 11/08/2004 regarding the restriction requirement in the previous Office Action has been fully considered but they are not persuasive. The traversal is on the grounds that Group I and Group II are clearly related and that a search for Group I would be relevant to the examination of Group II. This is not found persuasive because Group I is directed to a method for updating keys and Group II is directed to a method for authenticating messages. Groups I and II are related as subcombinations disclosed as usable together in a single combination and the subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, Group II has separate utility such as key generation. Because these inventions are distinct for the reasons given above ^{AND} the search required for one group is not required for the other group.

6B) The requirement is still deemed proper and is therefore made FINAL.

Art Unit: 2132

4. Claims 1-15 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected Group I, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 11/08/2004.

5. Applicant's arguments, see page 12, filed 11/08/2004, with respect to the rejection(s) of claim(s) 16, 25, 28 and 30 under 35 USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, a discovery of new prior art has necessitated new grounds of rejection. The delay in citation of the newly discovered prior art is regretted.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 16-19 and 23-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow (6,061,668) in view of Elgamal et al (5,825,890).

Regarding claim 16, Sharrow discloses a method comprising: applying at an appliance communication center an appliance message to an algorithm to generate a checksum value (fig. 2), and transmitting the appliance message and the checksum

value to the appliance (fig. 2). Sharrow does not disclose maintaining at the appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance, and applying both the appliance message and the shared message counter to the authentication algorithm to generate the first authentication word. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 24-30), applying both a message and a shared message counter to an authentication algorithm to generate a first authentication word (col. 17, line 56 – col. 18, line 6), and transmit the first authentication word with the message to a receiver (col. 18, lines 31-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the method of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance communication center and a remotely located appliance, to apply both the message and a shared message counter to an authentication algorithm to generate a first authentication word, and to transmit the first authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Regarding claim 17, Sharrow further discloses receiving the message at the appliance (fig. 2; col. 3, lines 23-26). Elgamal further discloses applying the shared message counter, as stored in the receiving side, and the received message to an authentication algorithm to generate a second authentication word and comparing the first and second authentication words to determine the authenticity of the message (col. 18, lines 31-38).

Regarding claim 18, Elgamal further discloses incrementing the shared message counter, as stored in the receiving side, after receiving a genuine authenticated message at the receiving side (col. 18, lines 24-33).

Regarding claim 19, Elgamal further discloses using a random number in combination with a sequence number, the random number meets the limitation of an authentication keying variable (col. 18, lines 20-23).

Regarding claim 23, Sharrow and Elgamal do not disclose maintaining a separate shared counter for a plurality of appliances. However, Sharrow discloses that the appliance communication center communicates with a plurality of appliances (fig. 1) and Elgamal discloses that the sequence numbers are specific to a particular pair of entities (col. 18, lines 24-27). Therefore, the feature is obvious by the combination of Sharrow and Elgamal as discussed in claim 16.

Regarding claim 24, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

Claims 25-26 are rejected on the same basis as claim 23.

Regarding claim 27, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

Claim 28 is rejected on the same basis as claim 17.

Claim 29 is rejected on the same basis as claim 18.

Regarding claim 30, Sharrow discloses a method comprising: applying an appliance message to an algorithm to generate a checksum value (fig. 3), and transmitting the appliance message and the checksum to an appliance communication center (fig. 3). Sharrow does not disclose maintaining at the appliance a shared message counter, the shared message counter shared between the appliance and the appliance communication center; and applying both the appliance message and the shared message counter to the authentication algorithm to generate the first authentication word. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 24-30), applying both a message and a shared message counter to an authentication algorithm to generate a first authentication word (col. 17, line 56 – col. 18, line 6), and transmit the first authentication word with the message to a receiver (col. 18, lines 31-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the method of Sharrow; in particular, it would have been

Art Unit: 2132

obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance and a remotely located communication center appliance, to apply both the message and a shared message counter to an authentication algorithm to generate a first authentication word, and to transmit the first authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Regarding claim 31, Sharrow further discloses receiving the message at the appliance communication center (fig. 2; col. 3, lines 23-26). Elgamal further discloses applying the shared message counter, as stored in the receiving side, and the received message to an authentication algorithm to generate a second authentication word and comparing the first and second authentication words to determine the authenticity of the message (col. 18, lines 31-38).

8. Claims 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Elgamal as applied to claim 19 above, and further in view of Kaufman et al ("Network Security Private Communication in a Public World"). Sharrow and Elgamal disclose using a shared message counter to generate the first authentication word in claim 16. Elgamal discloses that the authentication algorithm iteratively performs arithmetic or logical operations (col. 18, lines 4-6). Sharrow and Elgamal do not disclose using a directional code to generate the first authentication word, Kaufman teaches using a directional code for authentication (Section 9.3.5 Privacy and Integrity, p. 242, 3rd par). It would have been obvious to one of ordinary

Art Unit: 2132

skill in the art at the time the invention was made to modify the combined method of Sharrow and Elgamal to use a directional code for authentication, as taught by Kaufman. Accordingly, the directional code is used to generate the first authentication word. The motivation for doing so would have been to be able to prevent a reflection attack. Sharrow discloses a working register (col. 5, lines 1-5). Sharrow does not disclose that the working register comprising at least four bytes, the first three bytes holding the shared message counter the fourth byte holding the directional code. However, the differences between the claimed working register and the working register of Sharrow is a matter of design choice since both store the shared message counter and the directional code.

Allowable Subject Matter

9. Claims 21-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 21, the limitations "forming P as the dot product of R2 and R0; forming Q as the bitwise exclusive or of P with the constant expression '01010101'; forming S by adding Q to K; forming S' by end around rotating S; forming T as the bitwise exclusive or of S' and R3; forming F as the bitwise exclusive or of T with a byte of the appliance message; and replacing R3 with R2, R2 with R1, R1 with R0, and R0

Art Unit: 2132

with F", in combination with elements of the parent claims, have not been taught by prior art.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 4,918,728 to Matyas et al

U.S. Patent No. 6,055,316 to Perlman et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

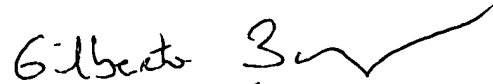
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 2132

MD

Minh Dinh
Examiner
Art Unit 2132

MD
3/20/05

A handwritten signature in black ink, appearing to read "Gilberto Barrón Jr.", with a stylized flourish extending to the right.

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100